72056-97339218@requests.muckrock.com (Anonymous requestor)
US mail to: MuckRock News, DEPT MR 72056, 411A Highland Ave, Somerville, MA 02144-2516
Please use email only. I am an anonymous user of MuckRock.com, not a MuckRock representative.

Sunshine Ordinance Task Force
Room 244
1 Dr. Carlton B. Goodlett Place
San Francisco CA 94102
sotf@sfgov.org
sent via email

Your ref.
SOTF 19044

Date
2019-06-04

RE: SF Sunshine Ordinance Complaint against City Attorney, 19044

To the Sunshine Ordinance Task Force:

NOTE: Every response you send or provide (including all responsive records) may be automatically and immediately visible to the general public on the MuckRock.com web service used to issue this request. (I am not a representative of MuckRock)

As an initial matter, the Respondents' response makes reference to me being affiliated with MuckRock. I want to be clear – I am not a MuckRock representative (as I state in many of my communications) and I do not speak for MuckRock News in any way; I am an anonymous person using MuckRock.com's FOIA management services open to the general public.

On May 8, 2019, I filed a Sunshine Ordinance complaint with your Task Force against the Office of the City Attorney, Dennis Herrera (city attorney), and Elizabeth Coolbrith (paralegal to city attorney), and sent a copy to the City Attorney by email as a courtesy.

On May 10, 2019, Cheryl Leger, Assistant Clerk, Board of Supervisors captioned my complaint *19044, Anonymous v. Dennis Herrera, Elizabeth Coolbrith* and requested from the Office of the City Attorney a response within 5 business days.

On May 17, 2019, I received an additional email from Ms. Coolbrith on behalf of the City Attorney disclosing additional portions of one of the records responsive to my request and requesting I withdraw my Task Force complaint. On the same day, I replied[1] to the City Attorney's office

[1] `https://cdn.muckrock.com/outbound_request_attachments/Anonymous_2859385/72056/`

and also forwarded my response to your Task Force for your files and consideration, outlining the reasons I do not believe the additional disclosures are legally sufficient, and asked that, even if your Task Force finds the additional disclosures sufficient, your Task Force still find the City Attorney's prior actions non-compliant with the Sunshine Ordinance. At the time of writing that reply I was not aware Respondents had replied to your Task Force. Please consider in your deliberations both my May 17 and this June 4 responses.

On June 3, 2019, I sent a followup to your Task Force requesting the Respondents' response if any. On June 4, 2019, Leger forwarded me a copy of the Respondents' May 17 response. I provide my rebuttal for your consideration below. Note that the issues concerned here are related, but not identical to, those in my complaint *19047, Anonymous v. Mayor London Breed, Hank Heckel, Office of Mayor*.

1. As background, while not binding upon your Task Force, consider this note from League of California Cities' "The People's Business"[2]:

   > Agencies that receive requests for metadata or requests for records that include metadata should treat the requests the same way they treat all other requests for electronic information and disclose nonexempt metadata.

   It also points out that "evolving law in other jurisdictions has held that local agency metadata is a public record subject to disclosure unless an exemption applies"[3] (see *Lake v. City of Phoenix*, (2009) 218 P.3d 1004, 1008; *O'Neill v. City of Shoreline* (2010) 240 P.3d 1149, 1154; *Irwin v. Onondaga County* (2010) 895 N.Y.S.2d 262, 268.).

2. Respondents state my possession of "Message-Ids" for the requested records indicates I may have access to the emails in native form myself. My understanding of email technology indicates that is not completely true. While I may have my "view" or "copy" of an email, that is not identical to the Respondents' copy. When you send an email message, that message ID is fixed as the email travels from the sender, their email server, any intermediate servers, the recipients' servers, etc, while the electronic record changes as it travels through those servers both gaining and losing certain information. For example, additional headers showing the intermediate servers may be added as the email travels to its recipient. However, certain other records may also be removed/hidden by those servers. For example, if Respondents 'bcc'-ed (blind carbon copied) their messages, the normal 'To' recipient won't see those Bcc headers, even though they are part of the public record, and would only be accessible from Respondents' original records.

3. Respondents argue they do not generally produce metadata, and that they suggest that City agencies do not need to do so in their "Good Government Guide." The Respondent's general practice not to provide metadata has no bearing on whether your task force should decide that metadata are, under the Sunshine Ordinance or CPRA, in fact, public records. I believe the "Good Government Guide" (which is itself written by and issued by Respondents) is

SF-Email-Appeal-72056-SOTF-19044-corrected-a.pdf

[2] Retrieved June 3, 2019. April 2017. League of California Cities. "The People's Business." Page 14. http://www.cacities.org/Resources/Open-Government/THE-PEOPLE%E2%80%99S-BUSINESS-A-Guide-to-the-California-Pu.aspx

[3] Ibid.

wrongly interpreting the CPRA and Sunshine Ordinance as argued in my complaint and in this rebuttal.

4. Note that the identity of authors and editors, draft changes, and comments shared, that the Good Government Guide (pg. 102) is concerned about in native documents (as opposed to PDF) are *not* excluded from disclosure by any specific Sunshine Ordinance provision. The common non-San Francisco responses of agencies to withhold draft and deliberative process documents are in fact specifically prohibited in most cases by SF Admin Code 67.24(a) and 67.24(h). Furthermore, if excluding that metadata *was* in fact legally acceptable and something San Francisco agencies should do, PDFs do not automatically solve the problem. PDFs can track changes, hold comments and author/editor identities, and contain substantial hidden metadata, unless it is excluded.

5. Respondents argue that metadata could create security risks or disclose privileged information. Respondents cite certain articles regarding hacking of the City of Atlanta and Baltimore systems, however the two articles do not seem to argue that such breaches were caused by disclosure of metadata. It is however the case that *certain* headers and similar could in fact create security risks, but this is not a blanket reason to withhold *all* headers or metadata.

6. Respondents argue they need to withhold "unique identifiers for our individual computer terminals and computer servers and our security certificates and similar information." To the extent that means IP addresses and certificate private keys are exempt under the Sunshine Ordinance, I do not disagree. These may in fact be justifiably withheld by redaction from responsive records.

7. To the extent that metadata could include attorney-client privilege, work product privilege, identity of a confidential whistleblower, or security information, that concern exists for the non-metadata "body" of any record as well. It is routinely redacted and handled correctly by City agencies, and it should be no different for metadata. The Respondents' May 17 disclosure is one example of doing this (albeit insufficient, as detailed in my May 17 response to your Task Force) – "print" to PDF the full email with headers, and redact those parts that are legally exempt.

8. Respondents state their decision to disclose even limited metadata is specific to this case. However, the Sunshine Ordinance makes public records public disclosable by default. Respondents should make their fact-specific judgement regarding which metadata is privileged or otherwise excluded in each case, and if the requestor has asked for metadata, justify the specific withholding as required by the Sunshine Ordinance.

9. Metadata and native formats include information that is both non-exempt and important. San Francisco does not permit its agencies to use the public interest balance exemption (SF Admin Code 67.24(g,i)), however, I thought it would be useful to explain why non-exempt metadata and native formats may be useful to the public. Native formats allow the public to easily search, index, import, and analyze information about the public business; PDFs create an additional barrier to making this information universally accessible as they are not optimized for email storage. Metadata that does not put the City at risk for security breaches and is not otherwise exempt include information such as which who actually sent an email

(the City Attorney, vs. his subordinates), when it was created and sent, if and when it was received. Metadata can help answer common investigative and journalistic questions including "who knew what, and when did they know it?"

10. There are ways for Respondents (and other City agencies) to both meet their requirements under the Sunshine Ordinance, CPRA, and California Constitution while protecting the City's security. One proposal I made in my May 17, 2019 followup to this complaint was[4]:

    > the City Attorney publishes an opinion that in its independent legal judgment, and in good faith consultation with information technology security experts, that all e-mail header names are non-exempt and at least the following e-mail header values (in addition to body, attachments and inline images) [Date, Sender, Message-Id, To, From, Subject, Mime-Version, Content-Type, Return-Path, Cc, Bcc, X-Envelope-From, Thread-Topic, Thread-Index, Sender, References, In-Reply-To, X-Originatororg, Delivered-To, X-Forwarded-To, X-Forwarded-For] are in fact not automatically exempt from disclosure (unless the specifc [sic] content is exempt);

    A similar process can be used for electronic records in general: that the City consult with IT security experts and provide uniform policies on which headers/metadata are genuinely exempt due to security concerns and directing that others can be safely released.

I hope that the complaint is now ripe for consideration by your Task Force or a committee thereof. As it would be difficult for me to be physically present at any in-person hearings, and in order to maintain my anonymity, I would appreciate the opportunity to be heard via conference call (telephone, Google Hangouts, Skype, etc.) if needed. Since this e-mail mailbox is completely public, I can send an email from a private address to retrieve conference call connection information if it is available.

Sincerely,

72056-97339218@requests.muckrock.com (Anonymous requestor)

[4] My May 17, 2019 follow-up to SOTF 19044, pg. 3, `https://cdn.muckrock.com/outbound_request_attachments/Anonymous_2859385/72056/SF-Email-Appeal-72056-SOTF-19044-corrected-a.pdf`